

Computer/Internet Use Policy

The internet provides a source of information that can benefit every profession and discipline represented at St. Stephens Indian School. It is the policy of the School that employees' job performance can be enhanced through the internet that is provided and becomes proficient with its capabilities. This policy document delineates acceptable use of the Internet by school employees, volunteers, and contractors while using government/school/school-owned or school-leased equipment, facilities, internet addresses, or domain names registered to St. Stephens Indian School.

Scope of the Policy

This policy applies to internet access only. It does not cover the requirements, standards, and procedures for the development and implementation of school information sites (Infinite Campus). The following internet users are covered by this policy:

- a. Full or part-time employees of St. Stephens Indian School.
- b. Volunteers who are authorized to use school resources to access the internet.
- c. School contractors/consultants who are authorized to use government/school-owned equipment or facilities.

This policy also distinguishes between internet access performed during normal working hours and access performed on personal time (on weekends, before and after work, during lunch periods, or during scheduled break period, etc.). This policy applies to internet access when using government/school equipment and facilities and when using Internet Protocol (IP) addresses and domain names registered to the school.

Policy

St. Stephens Indian School promotes internet use that enables employees to perform school missions and encourages its employees, volunteers, and contractors to develop internet skills and knowledge. Employees who do not require access to the internet as part of their official duties may not access the internet using school facilities under any circumstances. It is expected that employees will only use the internet to improve their job knowledge: to access scientific, technical, and other information on topics which have relevance to the school; and to communicate with their peers in other government/school agencies, academia, and industry. Users should be aware that when access is accomplished using school resources including the school network or when utilizing internet addresses and domain names registered to St. Stephens Indian School, such access may be perceived by others to represent the school. Users are advised not to use the internet for any purpose that would reflect negatively on the school or its employees. Federal computer systems are for school use and not for personal use; however, when certain criteria are met, school users are permitted to engage in the following activities:

- a. During working hours, access job-related information, as needed, to meet the requirements of their jobs.
- b. During working hours, participate in news groups, chat sessions, and email discussion groups (provided these sessions have a direct relationship to the user's job with the

school). If personal opinions are expressed, a disclaimer should be included stating that this is not an official position of the school.

- c. During personal time, retrieve non-job-related text and graphics information to develop or enhance internet-related text and graphics information. It is expected that these skills will be used to improve the accomplishment of job-related work assignments. This policy of allowing employees to use internet resources during non-work periods is similar to the policy of allowing staff to use library resources on personal time. The use of both types of resources enhances the employees' knowledge and skill in information retrieval, benefits which immediately translate to his or her ability to perform work-related activities. By encouraging employees to explore the internet, the school also builds its pool of internet-literate staff that can then guide and encourage other employees.
- d. Employees are prohibited from initiating internet sessions unrelated to work using school information resources from remote locations. That is, employees shall not dial into the school network or servers from any off-campus location for the purpose of participating in non-job related internet activities.

The following uses of the internet, either during working hours or personal time, using school equipment or facilities, are not allowed:

1. Accessing, retrieving, or printing of text and graphics information which exceeds the bounds of generally accepted standards of good taste and ethics.
2. Engaging in any unlawful activities or any other activities which would in any way bring discredit to St. Stephens Indian School.
3. Engaging in personal commercial activities on the internet, including offering/purchasing services or merchandise from on-line vendors.
4. Engaging in any activity which would compromise the security of any government/school host computer. Host log-in ID's and passwords shall not be disclosed or shared with anyone.
5. Engaging in any fundraising activity, endorsing any product or services, participating in any lobbying activity, or engaging in any active political activity.

Supervisory Responsibility

Supervisors of school employees, volunteers, and contractors have the final authority in determining whether an employee requires internet skills to accomplish their assigned duties.

Supervisors have the responsibility for:

- a. Acquiring Internet access for their employees if needed to conduct official business of the school.
- b. Determining whether or not internet access is provided to their employees for a flat fee. If access is provided on a flat fee basis, employees may use the internet for the activities outlined above. Supervisors should check with the online service provider of LAN administrator, as appropriate, to determine whether their internet access is acquired at a flat fee.
- c. Advising their employees regarding the restrictions against personal use of school internet access resources from other than school facilities.

- d. Assuming the responsibility for making the final determination as to the appropriateness of their employee's use of the internet when questions arise. This shall include the acceptability of the internet sites visited and the determination of personal time versus official work hours.

User Responsibilities

Use of computer equipment and internet access to accomplish job responsibilities always has priority over seasonal use. To avoid network capacity issues and to reduce the susceptibility of school information technology resources to computer viruses, internet users will comply with the following guidelines.

- a. Personal files, including those obtained via internet will not be stored on individual PC hard drives or on local area network (LAN) file servers. This includes personal e-mail, digital images, audio files, etc.
- b. Official video and audio files should not be downloaded from the internet except when they will be used to server an approved school function.
- c. B.I.E. security online training and certification is required.

Users Are Responsible For:

1. Following existing security policies and procedures in their use of internet services and will refrain from any practices, which might jeopardize the school's computer systems and data files, including but not limited to virus attacks, when downloading files from the internet.
2. Learning about internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
3. Familiarizing themselves with any special requirements for accessing, protecting, and utilizing data, including Privacy Act materials, copyrighted materials, and procurement sensitive data.
4. Conducting themselves in a way that reflects positively on the school, since they are identified as school employees on the internet even though they may be using the internet for personal reasons, as stated above.
5. Being aware, along with their supervisors, whether internet access is billed on a flat fee rather than a usage sensitive basis.

Individuals using government/school equipment to access the internet are subject to having activities monitored by system or security personnel. Use of this system constitutes consent to security monitoring, and employees should remember that most sessions are not private.